UNIVERSITY OF EDINBURGH

FACULTY OF SCIENCE AND ENGINEERING

COMPUTER SCIENCE FOUR

COMPUTER ALGEBRA

Friday 26 April 2002

09:30 to 11:00

Examiners:

Prof. K. Turner (External)

Prof. C. Stirling (Chairman)

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

1. (a) Explain what is meant by a *canonical representation* and a *normal representation* of objects. [*4 marks*]

(b) Explain how Maple represents rational numbers in a canonical form.

A naïve implementation of rational arithmetic results in computations with integers that are larger than necessary. Explain how we can improve matters for the multiplication and addition of rational numbers (division and subtraction are variants of these two cases and need not be discussed). [*6 marks*]

(c) Consider the following Maple code:

```
#   f,g,p .....   polynomials in x with rational coefficients
#                 where p is irreducible.
#   x .........   a name.
# Output:
#   View the arguments as specifying f(a)/g(a) for any root a
# of p.  If g(a) = 0 then an error is signalled.  Otherwise we
# return a polynomial r in the indeterminate x such that
# f(a)/g(a) = r(a) and r is either 0 or has degree strictly less
# than that of p.
# Assumptions:
#   The three polynomials are given in expanded form, and p is
# irreducible.
adiv:=proc(f,g,p,x)
  local u,v;
  if rem(g,p,x) = 0 then ERROR("attempt to divide by 0")
  else
    gcdex(g,p,x,u,v);
    rem(u*f,p,x)
  fi
end:
```

If $g(a) \neq 0$ then the code finds a polynomial u such that $ug \equiv 1 \pmod{p}$ so that u is the inverse of g in $\mathbb{Q}[x]/(p)$, the field obtained by carrying out arithmetic on polynomials from $\mathbb{Q}[x]$ but with all results taken modulo p. Thus u is the inverse of g in this field and $f/g = uf$.

i. What simple change to the procedure header would ensure a check by Maple that the parameter x is indeed a name when `adiv` is called? [*2 marks*]

ii. The code checks that $g(a) \neq 0$ by testing that p does not divide g. Justify this by proving that $g(a) = 0$ if and only if p divides g in $\mathbb{Q}[x]$. (You may assume without proof the fact that two polynomials have a common root in $\mathbb{C}$ if and only if they have a non-constant common factor in $\mathbb{Q}[x]$.) [*5 marks*]

QUESTION CONTINUES ON NEXT PAGE

iii. The efficiency of the code can be improved by observing that the test `rem`$(g, p, x) = 0$ could be replaced by a suitable test on the result of `gcdex`(g, p, x, u, v) (which is not used at all in the version of the code shown). State the test and justify it briefly. [*3 marks*]

iv. Assume that $g(a) \neq 0$ and let r be the result returned by `adiv`(f, g, p, x). Is $r(a)$ a canonical form for $f(a)/g(a)$? Justify your answer. [*5 marks*]

2. Let x be an indeterminate over $\mathbb{Z}$ and suppose throughout the question that $A, B \in \mathbb{Z}[x]$ are both non-zero with:

- $\deg(A) = n$,
- $\deg(B) = m$,
- $m \leq n$,
- the leading coefficient of B is 1.

If $H \in \mathbb{Z}[x]$ is either 0 or has degree at most r we define the polynomial

$$\mathrm{rev}_r(H) = x^r H(1/x).$$

Note that if $H = h_0 + h_1 x + \cdots + h_s x^s$ with $h_s \neq 0$ then $\mathrm{rev}_r(H) = (h_s + h_{s-1}x + \cdots + h_0 x^s)x^{r-s}$.

If G is any other polynomial and $i \geq 1$ is an integer we will use the notation

$$H \equiv G \pmod{x^i}$$

to mean, as usual, that x^i divides $H - G$, i.e., that the coefficients of H and G agree for all powers of x up to $i - 1$.

(a) Prove that there are $Q, R \in \mathbb{Z}[x]$ such that

$$A = QB + R$$

and either $R = 0$ or $\deg(R) < m$.
Deduce that $\deg(Q) = n - m$. *[8 marks]*

(b) Using the notation of the preceding part, prove that

$$\mathrm{rev}_n(A) \equiv \mathrm{rev}_{n-m}(Q)\,\mathrm{rev}_m(B) \pmod{x^{n-m+1}}.$$

Deduce that if we have a polynomial $C \in \mathbb{Z}[x]$ such that

$$C\,\mathrm{rev}_m(B) \equiv 1 \pmod{x^{n-m+1}}$$

then

$$\mathrm{rev}_{n-m}(Q) \equiv C\,\mathrm{rev}_n(A) \pmod{x^{n-m+1}}.$$

[7 marks]

QUESTION CONTINUES ON NEXT PAGE

(c) The following can be shown:

Fact. Suppose $f, g_0, g_1, \ldots \in \mathbb{Z}[x]$ with $f(0) = 1$, $g_0 = 1$ and

$$g_{i+1} \equiv 2g_i - fg_i^2 \pmod{x^{2^{i+1}}},$$

for all i. Then

$$fg_i \equiv 1 \pmod{x^{2^i}}$$

for all i.

This fact can be used to design a simple but efficient algorithm for deciding if B divides A which avoids polynomial division. The algorithm (with three gaps labelled E_1, E_2, E_3 and enclosed in angle brackets) is:

INPUT: A, B (satisfying the conditions above).
OUTPUT: TRUE if A divides B else FALSE.

$f := \langle E_1 \rangle$;
$g := 1$;
for i from 1 to $\lceil \lg(n - m + 1) \rceil$ do
  $g := \langle E_2 \rangle$;
od;
$Q := \mathrm{rev}_{n-m}(\mathtt{rem}(g\, \mathrm{rev}_n(A), x^{n-m+1})$;
if $\langle E_3 \rangle$ then TRUE else FALSE fi;

In the algorithm we use $\mathtt{rem}(H, x^i)$ to denote the polynomial obtained from H by keeping only those powers of x that have degree at most $i - 1$, e.g., $\mathtt{rem}(2 - 3x + x^2 - 5x^3 + x^4, x^3) = 2 - 3x + x^2$.

Provide appropriate expressions for E_1, E_2, E_3 and illustrate the algorithm by showing that $B = x^2 + 1$ divides the polynomial $A = 2x^3 - x^2 + 2x - 1$. [*10 marks*]

3. This question is concerned with Gröbner bases of ideals of polynomials with coefficients from a field k in a set of indeterminates $X = \{ x_1, x_2, \ldots, x_n \}$ where $n \geq 1$. Throughout let $G = \{ g_1, g_2, \ldots, g_m \}$ be a non-empty set of non-zero polynomials from $k[X]$ and $<$ a chosen admissible order on the set of power products in the indeterminates from X.

   (a) Explain what is meant by reduction with respect to G, i.e., explain what is denoted by the notation $f \to_G h$ for polynomials f, h. *[3 marks]*

   (b) Prove that if $f \to_G^* 0$ (where $\to_G^*$ denotes zero or more reduction steps) then f is in the ideal (G). *[3 marks]*

   (c) Give a counterexample to show that the converse of the preceding part is not necessarily true. *[3 marks]*

   (d) Recall that G is said to be a *Gröbner basis* for (G) if for every nonzero polynomial $h \in (G)$ there is a $g \in G$ such that $\operatorname{lpp}(g) \mid \operatorname{lpp}(h)$, where lpp denotes the leading power product of its argument with respect to the chosen order $<$. Suppose now that G is a Gröbner basis. Show that $f \to_G^* 0$ if and only if $f \in (G)$. *[5 marks]*

   (e) Prove that if $s_1, s_2, \ldots, s_m$ are power products then $\{ s_1, s_2, \ldots, s_m \}$ is a Gröbner basis of the ideal $(s_1, s_2, \ldots, s_m)$, with respect to any admissible order.

   Deduce that if s is a power product then $s \in (s_1, s_2, \ldots, s_m)$ if and only if $s_i \mid s$ for some i with $1 \leq i \leq m$. *[5 marks]*

   (f) For $1 \leq i \leq n$ let H_i denote the subset of k^n defined by the equation $x_i = 0$. For each non-empty subset S of $\{ 1, 2, \ldots, n \}$ set $K_S = \cup_{i \in S} H_i$, e.g., $K_{\{1,3,4\}} = H_1 \cup H_3 \cup H_4$. Suppose we are given non-empty subsets $S, S_1, S_2, \ldots, S_m$ of $\{ 1, 2, \ldots, n \}$. Assume now that k is algebraically closed. Prove that $K_{S_1} \cap K_{S_2} \cap \cdots \cap K_{S_m} \subseteq K_S$ if and only if $S_i \subseteq S$ for some i with $1 \leq i \leq m$. *[6 marks]*